UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/072,356	03/25/2011	Kwang Hyun Lim	79900-789745(065310US)	5821

66945 7590 01/19/2018

KILPATRICK TOWNSEND & STOCKTON LLP/VISA
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER
POLLOCK, GREGORY A

ART UNIT	PAPER NUMBER
3695	

NOTIFICATION DATE	DELIVERY MODE
01/19/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipefiling@kilpatricktownsend.com
EDurrell@kilpatricktownsend.com
KTSDocketing2@kilpatrick.foundationip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KWANG HYUN LIM and RICHARD LOUIS DELERY

Appeal 2016-005831
Application 13/072,356[1]
Technology Center 3600

Before ALLEN R. MacDONALD, JOSEPH P. LENTIVECH, and KARA L. SZPONDOWSKI, *Administrative Patent Judges*.

LENTIVECH, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 1–4 and 10–25. Claims 5–9 have been canceled. *See* App. Br. 32 (Claims App'x). We have jurisdiction over the pending claims under 35 U.S.C. § 6(b).

We affirm.

---

[1] According to Appellants, the real party in interest is Visa International Service Association. App. Br. 2.

STATEMENT OF THE CASE

Appellants' Invention

Appellants' invention generally relates to methods for detection and prevention of fraudulent transactions in payment processing networks. Spec. ¶¶ 5, 6. Claim 1, which is illustrative, reads as follows:

> 1. A method comprising:
>
> sending, by a computing device via a gateway, an automated alert message to a mobile device associated with a portable consumer device, wherein the automated alert message provides notification of a recent transaction between a merchant and a user related to an account that is associated with the portable consumer device;
>
> receiving, by the computing device via the gateway, a reply message in response to the automated alert message, wherein the reply message indicates that the recent transaction is fraudulent;
>
> updating, by the computing device, a risk engine with data associated with the reply message, wherein the risk engine comprises a risk scoring algorithm, and wherein the risk engine generates fraud scores for future payment transactions conducted by the user and other users utilizing peer group usage history, transaction histories of the user, and location data for transactions; and
>
> sending, by the computing device via the gateway, a notification regarding potential fraud based on an analysis by the risk engine of the data associated with the reply message;
>
> receiving transaction data for a subsequent transaction; and
>
> determining if the subsequent transaction is fraudulent using the transaction data for the subsequent transaction and the updated risk engine.

References

The Examiner relies on the following prior art in rejecting the claims:

Hillmer et al. ("Hillmer")	US 2003/0097330 A1	May 22, 2003
Bruesewitz et al. ("Bruesewitz")	US 2005/0149455 A1	July 7, 2005
Lakshminarayanan	US 2008/0275779 A1	Nov. 6, 2008
Chen et al. ("Chen")	US 8,805,737 B1	Aug. 12, 2014

Rejections

Claims 1–4 and 10–25 stand rejected under 35 U.S.C. § 101 as being directed to subject matter that is judicially-excepted from patent eligibility under § 101. Final Act. 2–3.

Claims 1–4, 10, 11, and 13–25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lakshminarayanan, Hillmer, and Chen. Final Act. 3–8.

Claim 12 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lakshminarayanan, Hillmer, Chen, and Bruesewitz. Final Act. 9.

ANALYSIS

§ 101 Rejection of Claims 1–4 and 10–25

In *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014), the Supreme Court reiterates an analytical two-step framework previously set forth in *Mayo Collaborative Servs. v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 77–78 (2012), "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice*, 134 S. Ct. at 2355. The first step in the analysis is to "determine whether the claims at issue are directed to one

of those patent-ineligible concepts," such as an abstract idea. *Alice*, 134 S. Ct. at 2355. If the claims are directed to a patent-ineligible concept, the second step in the analysis is to consider the elements of the claims "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Id.* (citing *Mayo*, 566 U.S. at 78–79). In other words, the second step is to "search for an 'inventive concept'—*i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* (citing *Mayo*, 566 U.S. at 72–73). We, therefore, look to whether the claims focus on a specific means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016).

In rejecting claims 1–4 and 10–23, the Examiner finds these claims are directed to "fraud detection." Final Act. 2. The Examiner finds fraud detection is a fundamental economic practice and, therefore, the claims are directed to an abstract idea. *Id.* The Examiner finds the claims do not recite "significantly more" than the abstract idea because "the claims do not include an improvement to another technology or technical field, an improvement to the functioning of the computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment" and "[t]he limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to perform generic computer functions that are

well-understood, routine and conventional activities previously known to the industry." Final Act. 2–3.

Appellants contend

> Assuming, *arguendo*, that the claims are directed to an alleged abstract idea of a "fraud detection," . . . the claims recite meaningful limitations that sufficiently limit the practical application of any alleged abstract idea of a "fraud detection" and thus do "not seek to tie up any judicial exception such that others cannot practice it" and thus constitute patent-eligible subject matter under 35 U.S.C. § 101.

App. Br. 10.

Appellants further contend the claims recite significantly more because the claims are necessarily rooted in computer technology to overcome a problem specifically arising in the realm of computer technology because the claims can utilize a number of different devices in a distributed system to prevent fraudulent transactions. App. Br. 11.

We find claims 1–4 and 10–25 are directed to fraud detection, a fundamental economic practice and, thus, an abstract idea. The claimed invention, as illustrated by claim 1, sends an automated alert message providing notification of a recent transaction between a merchant and a user to a mobile device; receives a reply message indicating the recent transaction is fraudulent; updates a risk with data associated with the reply message; sends a notification regarding potential fraud based on an analysis by the risk engine of the data associated with the reply message; receives transaction data for a subsequent transaction; and determines if the subsequent transaction is fraudulent using the transaction data for the subsequent transaction and the update risk engine. *See* App. Br. 31 (Claims Appendix). As Appellants' Specification explains, the invention relates to

"improved methods for detection and prevention of fraudulent transactions." Spec. ¶ 6; *see also* Spec. ¶¶ 8–9 (providing "[o]ne embodiment of the invention is directed to a method for improved fraud detection and warning . . . ." and "[a]nother embodiment is directed to further methods where the risk engine uses data from a reply message to identify other potential fraudulent transactions."). That the claimed method requires use of a computer system does not cause the claims to be directed to something other than an abstract idea, because the claimed steps can "be carried out in existing computers long in use, no new machinery being necessary." *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972). Our conclusion that the claims are directed to an abstract idea is buttressed by the fact that we see no reason why the method could not be performed manually using, at most, pen and paper. *See CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373 (Fed. Cir. 2011) ("[A] method that can be performed by human thought alone is merely an abstract idea."); *id.* at 1372 ("It is clear that unpatentable mental processes are the subject matter of claim 3. All of claim 3's method steps can be performed in the human mind, or by a human using a pen and paper."). For example, a person may receive a telephone call from a credit card company indicating that the person's credit card has been used in a recent transaction in a state other than the state the person currently resides. The person may inform the credit card company that they are not currently located within the other state and do not have any plans to travel there in the near future. The credit card company may contact the retailer at which the fraudulent transaction occurred and inform the retailer that the transaction is fraudulent. Additionally, the credit card company may make a note in a file for the person indicating that any future transactions

occurring in the other state are likely to be fraudulent. Upon receiving a subsequent transaction occurring in the other state, the credit card company may determine that the transaction is fraudulent based on the note in the file.

Accordingly, we find the claims are directed to an abstract idea and turn to the second step of the analysis to determine whether the claims recite "significantly more."

Regarding the second step of the analysis, Appellants contend

> Assuming, *arguendo*, that the claims are directed to an alleged abstract idea of a "fraud detection," . . . the claims recite meaningful limitations that sufficiently limit the practical application of any alleged abstract idea of a "fraud detection" and thus do "not seek to tie up any judicial exception such that others cannot practice it" and thus constitute patent-eligible subject matter under 35 U.S.C. § 101.

App. Br. 10.

According to Appellants, "[t]he basis for the 'significantly more' prong of the test is exactly directed to the question of whether a patentee seeks to preempt or monopolize the exception." App. Br. 16. Appellants argue, therefore, because the claims do not pre-empt "any and all methods for 'real-time alerts for fraud detection'" the claims "constitute 'signficantly more' than the abstract idea. App. Br. 15–16.

We do not find Appellants' contention persuasive. Considerations for determining whether a claim with additional elements amounts to "significantly more" than the judicial exception itself include improvements to another technology or technical field *(Alice Corp.,* 134 S. Ct. at 2359 (citing *Diamond v. Diehr,* 450 U.S. 175, 177–78 (1981))); adding a specific limitation other than what is well-understood, routine and conventional in the field, or adding unconventional steps that confine the claim to a

particular useful application *(Mayo,* 132 S. Ct. at 1299, 1302); or other meaningful limitations beyond generally linking the use of the judicial exception to a particular technological environment *(Alice Corp.,* 134 S. Ct. at 2360). "While preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015). "Where a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, as they are in this case, preemption concerns are fully addressed and made moot." *Id.*

Appellants further contend the claims recite significantly more than the abstract idea because the claims are necessarily rooted in computer technology to overcome a problem specifically arising in the realm of computer technology because the claims can utilize a number of different devices in a distributed system to prevent fraudulent transactions. App. Br. 11 (citing *DDR Holdings, LLC v. Hotels.com*, 773 F.3d 1245 (Fed. Cir. 2014)). Appellants argue "the recited claims clearly 'apply the judicial exception with, or by use of, a particular machine,' as these claims recite the use of a computing device, as well as additional devices." App. Br. 14. Appellants further argue the claimed embodiments "improve the functioning of the computer itself" and "[t]he system is improved over conventional systems because conventional systems cannot provide for such up to date risk engines and cannot prevent the occurrence of subsequent electronic payment transaction fraud as in embodiments of the invention." *Id.*

We do not find Appellants' contention persuasive. Although the claimed subject matter evokes the use of a computer system to facilitate detecting fraudulent transactions, the functions performed by the computer

system in carrying out the recited steps are conventional, well-understood, and do not go beyond those of a general purpose computer. Therefore, the claimed subject matter merely recites the performance of a business practice known from the pre-Internet era, and it is not necessarily rooted in computer technology. *See OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362 (Fed. Cir. 2015) ("method of pricing a product for sale" and "apparatus for use in electronic commerce" relate to the concept of "offer based pricing" similar to other fundamental economic concepts found to be abstract ideas). "[M]erely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea." *See Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015). As such, we agree with the Examiner that the claims do not recite "significantly more" than the abstract idea.

Because Appellants' claims 1–4 and 10–25 are directed to a patent-ineligible abstract idea, and do not recite something "significantly more" under the second prong of the *Alice* analysis, we sustain the Examiner's rejection of these claims under 35 U.S.C. § 101.

Rejection of claims 1–4 and 10–25 under 35 U.S.C. § 103

CLAIM 1

Appellants contend the combination of Lakshminarayanan, Hillmer, and Chen fail to teach or suggest "sending, by the computing device via the gateway, a notification regarding potential fraud based on an analysis by the risk engine of the data associated with the reply message," as recited in claim 1. App. Br. 19–21; Reply Br. 14–15.

> Regarding the disputed limitation, the Examiner finds
>
> Figure 12 of Lakshminarayanan is labeled "Mobile Fraud Notification" (emphasis added). Additionally, it is clear that the Mobile Fraud Notification is sent to the Consumer Wireless Client (Figure 12, element 1202a) through a Payment Gateway (Figure 12, element 1208). Regarding applicant's argument that the notification is not sent bases on fraud analysis, this is not correct. Figure 12, element 1222 "allows data entry by the consumer of the amount of money that will trip an alert being sent to the cell phone ([¶86]).

Ans. 9.

Appellants argue Lakshminarayanan "does not even describe analyzing data associated with a reply message, let alone sending subsequent messages with information 'regarding potential fraud' based on an analysis of data associated with the reply message." App. Br. 20–21. According to Appellants, Lakshminarayan, instead, teaches sending an alert to a consumer wireless client. App. Br. 20 (citing Lakshminarayanan ¶ 93). Appellants argue providing basic alert triggers (e.g., an amount of money that will trip an alert) is not the same as sending a notification regarding potential fraud based on an analysis by the risk engine of the data associated with the reply message, as required by claim 1. Reply Br. 15. Appellants further argue the Examiner's reliance on the same alert message for teaching both sending "an automated alert message" and "a notification regarding claimed fraud," as required by claim 1 is improper because "the 'notification' and the 'automated alert message' are two different messages sent at different times, [so] they cannot both be taught or suggested by one consumer alert described in Lakshminarayanan." App. Br. 20.

We find Appellants' arguments persuasive. Lakshminarayanan teaches "allow[ing] a consumer to specify when and how they would like to

be notified that fraud is being conducted on an account issued by an issuer to the consumer" and that "[t]hese notifications can be sent to the consumer's cell phone in real time and in a variety of formats . . . thereby allowing the consumer to receive a general fraud alert in real time with the occurrence of the fraudulent transaction." Lakshminarayanan ¶ 89; *see also* Lakshminarayanan, Fig. 12. Figure 12 of Lakshminarayanan indicates that, in response to receiving the fraud alert, some form of a reply is provided by the consumer wireless client to the real-time anti-fraud detection system. Lakshminarayanan, Fig. 12. However, the Examiner's findings are insufficient to show that Lakshminarayanan teaches sending a second message (e.g., a notification regarding potential fraud) based on data associated with the reply, as required by claim 1. The Examiner does not find that the teachings of Hillmer and Chen cure the deficiencies in the teachings of Lakshminarayanan. As such, the Examiner's findings are insufficient to show that the combination of Lakshminarayanan, Hillmer, and Chen teaches or suggests the disputed limitation.

Accordingly, we do not sustain the Examiner's rejection under 35 U.S.C. § 103 of claim 1; independent claim 16, which recites similar limitations; and claims 2–4, 10–15, and 17–25, which depend from claims 1 and 16. Appellants' arguments regarding the rejection of claims 1–4 and 10–25 raise additional issues which we do not reach because we find this issue to be dispositive.

DECISION

We affirm the Examiner's rejection of claims 1–4 and 10–25 under 35 U.S.C. § 101.

We reverse the Examiner's rejection of claims 1–4 and 10–25 under 35 U.S.C. § 103(a).

Since at least one rejection encompassing all claims on appeal is affirmed, the decision of the Examiner is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED